

# A unified approach to autocorrelation of Frank, Chu, and Milewski sequences

Idris Mercer  
Florida International University  
imercer@fiu.edu

## Abstract

We construct a family of perfect polyphase sequences that has the Frank sequences, Chu sequences, and Milewski sequences as special cases. This is not the most general construction of this type, but it has a particularly simple form. We also include some remarks about the acyclic autocorrelations of our sequences.

## 1 Introduction

A **complex sequence** of **length**  $N$  is an  $N$ -tuple

$$\mathcal{X} = (\xi_0, \xi_1, \dots, \xi_{N-1})$$

where each  $\xi_j$  is a complex number of modulus 1. If furthermore each  $\xi_j$  is a  $D$ th root of unity, then the sequence is called a  **$D$ -phase sequence**, or **polyphase sequence** if we don't specify the value of  $D$ . Throughout this article, lowercase Greek letters will denote complex numbers and nonbold Latin letters will denote nonnegative integers, unless otherwise stated.

If  $0 \leq k \leq N - 1$ , we define the **acyclic autocorrelations** of  $\mathcal{X}$  by

$$\alpha_k = \sum_{j=0}^{N-k-1} \overline{\xi_j} \xi_{j+k}$$

and we define the **cyclic autocorrelations** of  $\mathcal{X}$  by

$$\gamma_k = \sum_{j=0}^{N-1} \overline{\xi_j} \xi_{j+k}$$

where the bar denotes complex conjugation, and in the definition of  $\gamma_k$ , the addition in the subscript is mod  $N$ , or equivalently, we assume  $\xi_j$  is defined for  $j \geq N$  by  $\xi_{j+N} = \xi_j$ .

Note that  $\alpha_k$  is a sum of  $N-k$  terms, each of modulus 1. Hence  $|\alpha_k| \leq N-k$ . Also note that if  $1 \leq k \leq N-1$ , we have  $\gamma_k = \alpha_k + \overline{\alpha_{N-k}}$ . It follows that if  $\gamma_k = 0$ , then  $|\alpha_k| = |\alpha_{N-k}| \leq k$ .

We can regard  $\alpha_k$  and  $\gamma_k$  as measuring resemblance between the sequence  $\mathcal{X}$  and a version of  $\mathcal{X}$  that has been shifted by  $k$  positions (acyclically or cyclically respectively). We have  $\alpha_0 = \gamma_0 = N$ , which we may call the **trivial** autocorrelations. Informally, we consider a sequence to be “good” if its nontrivial autocorrelations are close to 0 (so it is “uncorrelated” with shifted versions of itself.)

How close to 0 can we make the cyclic autocorrelations, and how close to 0 can we make the acyclic autocorrelations? The first of those questions has an easier answer than the second.

We call  $\mathcal{X}$  a **perfect** sequence if  $\gamma_k = 0$  for all  $k \neq 0$ . Many families of perfect sequences have been studied, including Frank sequences [4], Chu sequences [2], and Milewski sequences [6]. There are perfect sequences of every length  $N \geq 2$ . For a good recent survey of perfect sequences, see [11, Section 4.1].

We define the **peak sidelobe level** (abbreviated “PSL”) of  $\mathcal{X}$  by

$$\mathbf{P}(\mathcal{X}) = \max_{1 \leq k \leq N-1} |\alpha_k|,$$

and we define the **energy** of  $\mathcal{X}$  by

$$\mathbf{E}(\mathcal{X}) = \sum_{k=1}^{N-1} |\alpha_k|^2,$$

which are two natural measures of the “size” of the acyclic autocorrelations. A complex sequence with PSL at most 1 (i.e., with  $|\alpha_k| \leq 1$  for all  $k \neq 0$ ) is called a **generalized Barker sequence**. There exist generalized Barker sequences of all lengths  $N \leq 70$  (see [9]), and it has been conjectured that they exist for all lengths. See [11, Question 4.10] or [1, p. 119].

A generalized Barker sequence of length  $N$  has energy at most  $N - 1$ . But if we want an infinite family of complex sequences of increasing lengths  $N$  that have small energy, the best known infinite families (which are the Chu sequences and Frank sequences) have energy growing like  $O(N^{3/2})$ . See [10].

The **merit factor** of a length  $N$  complex sequence  $\mathcal{X}$  is defined by

$$\mathbf{F}(\mathcal{X}) = \frac{N^2}{2\mathbf{E}(\mathcal{X})}$$

so asking for small energy is equivalent to asking for large merit factor. The energy and merit factor are related to the  $L^4$  norm on the unit circle of the polynomial whose coefficients are the  $\xi_j$  (specifically, minimizing the energy of the sequence is equivalent to minimizing the  $L^4$  norm of the polynomial). See [1, Chapter 15].

We will construct a family of perfect polyphase sequences that contains the Frank sequences, Chu sequences, and Milewski sequences as special cases. This is not the most general construction of this type. In 1995, Mow provided a construction that included all known infinite families of perfect polyphase sequences [7]. For more discussion of families of perfect polyphase sequences, see [3].

Our family of sequences is not as general as Mow's, but it includes several well-known families in one surprisingly simple form. We will refer to our sequences as “LM sequences”, where LM could stand for “like Mow” but also names two integer parameters we use.

Some facts are already known about acyclic autocorrelation of families of perfect sequences. Turyn [12] showed that the PSL of the Frank sequence of length  $N$  is asymptotically equal to  $(1/\pi)\sqrt{N}$ . Mow and Li [8] showed that the PSL of the Chu sequence of length  $N$  is asymptotically equal to  $C\sqrt{N}$  for a slightly larger constant. The current author [5] showed that the energy of the Chu sequence of length  $N$  is bounded above by  $(8/3\pi^{3/2})N^{3/2}$ ; this was improved by Schmidt [10] who showed that the energy of the Chu sequence of length  $N$  is asymptotically equal to  $(1/\pi)N^{3/2}$ , and the energy of the Frank sequence of length  $N$  is asymptotically equal to  $(2/\pi^2)N^{3/2}$ . It appears that less is known about the PSL or energy of Milewski sequences.

For a good summary of acyclic autocorrelation of polyphase sequences, see [11, Section 4.2].

In this article, we do not say much about the acyclic autocorrelations of our sequences. As consequences of the proofs that our sequences are perfect sequences, it will follow that the Frank sequence of length  $N$  has PSL at most  $\sqrt{N/2}$ , and the Chu sequence of length  $N$  has PSL at most  $\sqrt{N}$ , which are slightly weaker than known results. The current author conjectures that there exist polyphase sequences of all lengths  $N$  whose energy grows like  $o(N^{3/2})$ . Perhaps further study of acyclic autocorrelations of general families of perfect sequences will prove this conjecture.

We note that if  $\mathcal{X}$  is a  $D$ -phase sequence, then each  $\xi_j$  can be written as  $\zeta_D^{p(j)}$ , where  $\zeta_D = e^{2\pi i/D}$  and  $p(j)$  belongs to the integers mod  $D$ . We can specify the sequence by specifying the values of  $p(j)$ .

## 2 LM sequences

Throughout the rest of this article,  $L$  and  $M$  are positive integers such that  $L$  divides  $M$ , and  $N$  denotes  $LM$ . Since  $N = 1$  is uninteresting, we assume  $M \geq 2$ . We will construct a  $2M$ -phase sequence of length  $N$ , informally consisting of  $M$  “blocks” each of length  $L$ . As before,  $\zeta_D$  means  $e^{2\pi i/D}$ .

For all nonnegative integers  $j$ , we define

$$s_j = \left\lfloor \frac{j}{L} \right\rfloor \quad \text{and} \quad t_j = j - L \left\lfloor \frac{j}{L} \right\rfloor.$$

Then  $j = s_j L + t_j$ . One can verify that  $s_{j+N} = s_j + M$  and  $t_{j+N} = t_j$ .

**Proposition 2.1.** Let  $L, M$  be as above, and let  $A$  be an integer with the same parity as  $LM$ . Define a function on the nonnegative integers as follows:

$$p(j) = 2s_j t_j + L s_j^2 + A s_j.$$

Then  $p$  is an integer-valued function that satisfies  $p(j + N) \equiv p(j) \pmod{2M}$ .

*Proof.* We have

$$\begin{aligned}
p(j+N) &= 2s_{j+N}t_{j+N} + Ls_{j+N}^2 + As_{j+N} \\
&= 2(s_j + M)t_j + L(s_j + M)^2 + A(s_j + M) \\
&= 2s_jt_j + 2Mt_j + Ls_j^2 + 2LMs_j + LM^2 + As_j + AM \\
&= p(j) + 2M(t_j + Ls_j) + M(LM + A)
\end{aligned}$$

and since  $LM + A$  is even, this proves the proposition.

It follows that if we define, for all  $j$ ,

$$\xi_j = \zeta_{2M}^{p(j)},$$

then we have  $\xi_{j+N} = \xi_j$  for all  $j$ .

**Definition 2.2.** We define the **LM sequence** of length  $N = LM$  to be

$$\mathcal{X} = (\xi_0, \xi_1, \dots, \xi_{N-1})$$

where  $\xi_j = \zeta_{2M}^{p(j)}$  and  $p(j)$  is as defined previously.

The sequence depends on our choice of  $L$ ,  $M$ , and  $A$ . (Recall we must have  $L|M$ , and  $A \equiv LM \pmod{2}$ .) We single out some important special cases.

**Special case (i).** If  $M$  is even, choose  $A = M$ , and if  $M$  is odd, choose  $A = L$ . We then have

$$p(j) = \begin{cases} 2s_jt_j + Ls_j^2 + Ms_j & \text{if } M \text{ is even,} \\ 2s_jt_j + Ls_j^2 + Ls_j & \text{if } M \text{ is odd.} \end{cases}$$

**Special case (ii).** If  $M$  is even, choose  $A = 0$ , and if  $M$  is odd, choose  $A = L$ . We then have

$$p(j) = \begin{cases} 2s_jt_j + Ls_j^2 & \text{if } M \text{ is even,} \\ 2s_jt_j + Ls_j^2 + Ls_j & \text{if } M \text{ is odd.} \end{cases}$$

**Special case (i)a.** Consider the subcase of special case (i) where  $M = L$ . Then  $N = M^2$ , and we have

$$p(j) = 2s_jt_j + Ms_j^2 + Ms_j = 2s_jt_j + Ms_j(s_j + 1).$$

Since  $s_j(s_j + 1)$  is even, we have  $p(j) \equiv 2s_j t_j \pmod{2M}$ . We then have

$$\xi_j = \zeta_{2M}^{p(j)} = \zeta_{2M}^{2s_j t_j} = \zeta_M^{s_j t_j}$$

which means  $\mathcal{X} = (\xi_0, \dots, \xi_{N-1})$  is the sequence of length  $M^2$  defined by

$$\xi_j = \xi_{s_j M + t_j} = \zeta_M^{s_j t_j}$$

which is equivalent to the Frank sequence of length  $M^2$  as defined in [4] or [11, Section 4.1].

**Special case (ii)a.** Consider the subcase of special case (ii) where  $L = 1$ . Then  $N = M$ , and we have

$$p(j) = \begin{cases} 2s_j t_j + s_j^2 & \text{if } M \text{ is even,} \\ 2s_j t_j + s_j^2 + s_j & \text{if } M \text{ is odd.} \end{cases}$$

If  $L = 1$ , then  $s_j = \lfloor j/1 \rfloor = j$  and  $t_j = j - 1j = 0$ , so the above becomes

$$p(j) = \begin{cases} j^2 & \text{if } M \text{ is even,} \\ j^2 + j & \text{if } M \text{ is odd.} \end{cases}$$

This means  $\mathcal{X} = (\xi_0, \dots, \xi_{N-1})$  is the sequence of length  $M$  defined by

$$\xi_j = \zeta_{2M}^{p(j)} = \begin{cases} \zeta_{2M}^{j^2} & \text{if } M \text{ is even,} \\ \zeta_{2M}^{j^2+j} = \zeta_M^{(j^2+j)/2} & \text{if } M \text{ is odd,} \end{cases}$$

which is equivalent to the Chu sequence of length  $M$  as defined in [2] or [11, Section 4.1].

**Special case (ii)b.** Consider the subcase of special case (ii) where  $L = G^H$  and  $M = G^{H+1}$ , where  $H > 0$ . Then  $N = G^{2H+1}$ , and we have

$$p(j) = \begin{cases} 2s_j t_j + G^H s_j^2 & \text{if } G \text{ is even,} \\ 2s_j t_j + G^H (s_j^2 + s_j) & \text{if } G \text{ is odd.} \end{cases}$$

This means  $\mathcal{X} = (\xi_0, \dots, \xi_{N-1})$  is the sequence of length  $G^{2H+1}$  defined by

$$\xi_j = \xi_{s_j G^H + t_j} = \begin{cases} \zeta_{2M}^{2s_j t_j + G^H s_j^2} = \zeta_M^{s_j t_j + \frac{G^H}{2} s_j^2} & \text{if } G \text{ is even,} \\ \zeta_{2M}^{2s_j t_j + G^H (s_j^2 + s_j)} = \zeta_M^{s_j t_j + G^H \frac{s_j^2 + s_j}{2}} & \text{if } G \text{ is odd,} \end{cases}$$

or equivalently,

$$\xi_j = \xi_{s_j G^H + t_j} = \begin{cases} \exp\left(\frac{2\pi i}{G^{H+1}}(s_j t_j + \frac{G^H}{2} s_j^2)\right) & \text{if } G \text{ is even,} \\ \exp\left(\frac{2\pi i}{G^{H+1}}(s_j t_j + G^H \frac{s_j^2 + s_j}{2})\right) & \text{if } G \text{ is odd,} \end{cases}$$

which is equivalent to the Milewski sequence of length  $G^{2H+1}$  as defined in [6] or [11, Section 4.1].

### 3 Useful lemmas

As always,  $\zeta_D$  denotes  $e^{2\pi i/D}$ . In this section,  $x$  denotes a real number.

**Lemma 3.1.** If  $a$  and  $k$  are any integers and  $k$  is not a multiple of  $D$ , then

$$\sum_{j=a}^{a+D-1} \zeta_D^{kj} = 0.$$

Proof: This sum of  $D$  terms is invariant under multiplication by  $\zeta_D^k \neq 1$ .

Lemma. We have  $|1 - e^{ix}| = 2 \left| \sin \frac{x}{2} \right|$ .

Proof:  $|1 - e^{ix}|^2 = (1 - \cos x)^2 + \sin^2 x = 2 - 2 \cos x = 4 \sin^2 \frac{x}{2}$ .

Lemma. If  $0 < x \leq \frac{\pi}{2}$  then  $\csc x \leq \frac{\pi}{2x}$ .

Proof: If  $0 < x \leq \frac{\pi}{2}$ , we have  $\sin x \geq \frac{2}{\pi}x > 0$ , and taking reciprocals proves the lemma.

Lemma. If  $\omega = e^{ix} \neq 1$ , and  $a < b$  are integers, then

$$|\omega^a + \omega^{a+1} + \dots + \omega^{b-1}| \leq \left| \csc \frac{x}{2} \right|.$$

Proof: If  $S = \omega^a + \omega^{a+1} + \dots + \omega^{b-1}$ , we have  $S - \omega S = \omega^a - \omega^b$  and so

$$|S| = \frac{|\omega^a - \omega^b|}{|1 - \omega|} = \frac{|e^{iax} - e^{ibx}|}{|1 - e^{ix}|} \leq \frac{2}{|1 - e^{ix}|} = \frac{2}{2 \left| \sin \frac{x}{2} \right|} = \left| \csc \frac{x}{2} \right|.$$

**Corollary 3.2.** If  $k$  is not a multiple of  $D$ , then taking  $\omega = \zeta_D^k = e^{i(2\pi k/D)} \neq 1$ , we get

$$\left| \sum_{j=a}^{b-1} \zeta_D^{kj} \right| \leq \left| \csc \frac{\pi k}{D} \right|.$$

If furthermore we have  $0 < k < D$ , this becomes

$$\left| \sum_{j=a}^{b-1} \zeta_D^{kj} \right| \leq \csc \frac{\pi k}{D}.$$

**Definition.** For positive integers  $k$  and  $D$ , let  $\delta(k, D)$  be the distance from  $k$  to the nearest multiple of  $D$ . So if  $k$  belongs to an interval of the form  $[jD, (j + \frac{1}{2})D]$ , then  $k = jD + \delta(k, D)$ , and if  $k$  belongs to an interval of the form  $[(j - \frac{1}{2})D, jD]$ , then  $k = jD - \delta(k, D)$ . For example,  $\delta(19, 12) = \delta(29, 12) = 5$ .

**Fact.** The function  $f(x) = \left| \csc \frac{\pi x}{D} \right|$  is periodic with period  $D$  and is symmetric on the interval  $[0, D]$ , i.e.  $f(D - x) = f(x)$ .

**Corollary 3.3.** If  $k$  is not a multiple of  $D$ , and  $k' = \delta(k, D)$ , then

$$\left| \csc \frac{\pi k}{D} \right| = \csc \frac{\pi k'}{D}$$

and furthermore, since  $0 < k' \leq \frac{D}{2}$ , we have

$$\left| \csc \frac{\pi k}{D} \right| \leq \frac{D}{2k'}.$$

## 4 Autocorrelation of LM sequences

Throughout this section,  $\mathcal{X} = (\xi_0, \dots, \xi_{N-1})$  is the LM sequence of length  $N$  defined previously. So  $L$ ,  $M$ ,  $A$ , and  $p(j)$  are as defined previously, and the autocorrelations  $\gamma_k$  and  $\alpha_k$  are sums of terms of the form

$$\overline{\xi_j} \xi_{j+k} = \zeta_{2M}^{p(j+k) - p(j)}.$$



Suppose  $1 \leq k \leq N - 1$ . We want to show  $\gamma_k = 0$ , and we want bounds on the size of  $\alpha_k$ .

Note that either  $k$  and  $N - k$  are both multiples of  $L$ , or  $k$  and  $N - k$  are both nonmultiples of  $L$ .

**Proposition 4.1.** Let  $\mathcal{X} = (\xi_0, \dots, \xi_{N-1})$  be the LM sequence of length  $N = LM$  defined previously. Suppose  $1 \leq k \leq N - 1$ , and suppose  $k$  and  $N - k$  are both multiples of  $L$ . Then the autocorrelations  $\gamma_k$  and  $\alpha_k$  satisfy  $\gamma_k = 0$  and  $|\alpha_k| \leq \sqrt{N/2}$ .

*Proof.* If  $k$  and  $N - k$  are both multiples of  $L$ , let  $k = qL$  and let  $N - k = rL$ . So  $q + r = M$ , and  $1 \leq q \leq M - 1$ . We break the sums  $\gamma_k$  and  $\alpha_k$  into sums of  $L$  terms:

$$\begin{aligned}\gamma_k &= \sum_{j=0}^{ML-1} \bar{\xi}_j \xi_{j+k} = \sum_{i=0}^{M-1} \sum_{j=iL}^{(i+1)L-1} \bar{\xi}_j \xi_{j+k}, \\ \alpha_k &= \sum_{j=0}^{rL-1} \bar{\xi}_j \xi_{j+k} = \sum_{i=0}^{r-1} \sum_{j=iL}^{(i+1)L-1} \bar{\xi}_j \xi_{j+k}.\end{aligned}$$

CLAIM 1: If  $iL \leq j \leq (i+1)L - 1$  and  $k = qL$  as above, then

$$p(j+k) - p(j) = 2qj + Lq^2 + Aq$$

which is of the form  $2qj + c_1$  where  $c_1$  is independent of  $i$  and  $j$ .

Claim 1 is proved in the appendix.

We then have

$$\begin{aligned}\gamma_k &= \sum_{i=0}^{M-1} \sum_{j=iL}^{(i+1)L-1} \zeta_{2M}^{p(j+k)-p(j)} = \zeta_{2M}^{c_1} \sum_{i=0}^{M-1} \sum_{j=iL}^{(i+1)L-1} \zeta_{2M}^{2qj} \\ &= \zeta_{2M}^{c_1} \sum_{j=0}^{ML-1} \zeta_{2M}^{2qj} = \zeta_{2M}^{c_1} \sum_{i=0}^{L-1} \sum_{j=iM}^{(i+1)M-1} \zeta_{2M}^{2qj} \\ &= \zeta_{2M}^{c_1} \sum_{i=0}^{L-1} \sum_{j=iM}^{(i+1)M-1} \zeta_M^{qj} = \zeta_{2M}^{c_1} \sum_{i=0}^{L-1} 0 = 0\end{aligned}$$

where we have used Lemma 3.1 and the fact that  $q$  is not a multiple of  $M$ . We also have

$$\alpha_k = \sum_{i=0}^{r-1} \sum_{j=iL}^{(i+1)L-1} \zeta_{2M}^{p(j+k)-p(j)} = \zeta_{2M}^{c_1} \sum_{i=0}^{r-1} \sum_{j=iL}^{(i+1)L-1} \zeta_{2M}^{2qj} = \zeta_{2M}^{c_1} \sum_{j=0}^{rL-1} \zeta_{2M}^{2qj}$$

which implies

$$|\alpha_k| = \left| \sum_{j=0}^{rL-1} \zeta_{2M}^{2qj} \right| = \left| \sum_{j=0}^{rL-1} \zeta_M^{qj} \right| \leq \csc \frac{\pi q}{M} = \csc \frac{\pi(k/L)}{M} = \csc \frac{\pi k}{N}$$

where we have used Corollary 3.2 and the fact that  $0 < q < M$ .

Since  $\gamma_k = 0$ , we know  $|\alpha_k| = |\alpha_{N-k}|$ . Therefore when bounding  $|\alpha_k|$ , it suffices to consider  $k \leq N/2$ . If  $1 \leq k \leq \sqrt{N/2}$ , then  $|\alpha_k| \leq k \leq \sqrt{N/2}$ . If  $\sqrt{N/2} \leq k \leq N/2$ , then

$$|\alpha_k| \leq \csc \frac{\pi k}{N} \leq \frac{N}{2k} \leq \frac{N}{2\sqrt{N/2}} = \sqrt{\frac{N}{2}}$$

which completes the proof of Proposition 4.1.

**Proposition 4.2.** Let  $\mathcal{X} = (\xi_0, \dots, \xi_{N-1})$  be the LM sequence of length  $N = LM$  defined previously. Suppose  $1 \leq k \leq N-1$ , and suppose  $k$  and  $N-k$  are both nonmultiples of  $L$ . Then the autocorrelation  $\gamma_k$  satisfies  $\gamma_k = 0$ . Furthermore, in the special case  $L = M$ , the autocorrelation  $\alpha_k$  satisfies  $|\alpha_k| \leq M = \sqrt{N}$ .

*Proof.* If  $k$  and  $N-k$  are both nonmultiples of  $L$ , let  $k = qL + k_1$  and let  $N-k = rL + k_2$ , where  $1 \leq k_1, k_2 \leq L-1$  and  $k_1 + k_2 = L$ . So  $q+r = M-1$ . We break the sums  $\gamma_k$  and  $\alpha_k$  into sums of  $k_1$  terms and sums of  $k_2$  terms:

$$\begin{aligned} \gamma_k &= \sum_{i=0}^{M-1} \sum_{j=iL}^{iL+k_2-1} \bar{\xi}_j \xi_{j+k} + \sum_{i=0}^{M-1} \sum_{j=iL+k_2}^{(i+1)L-1} \bar{\xi}_j \xi_{j+k}, \\ \alpha_k &= \sum_{i=0}^r \sum_{j=iL}^{iL+k_2-1} \bar{\xi}_j \xi_{j+k} + \sum_{i=0}^{r-1} \sum_{j=iL+k_2}^{(i+1)L-1} \bar{\xi}_j \xi_{j+k}. \end{aligned}$$

CLAIM 2: If  $iL \leq j \leq iL + k_2 - 1$  and  $k = qL + k_1$  where  $k_1, k_2$  are as above, then

$$p(j+k) - p(j) = 2ik_1 + 2qj + 2qk_1 + Lq^2 + Aq$$

which is of the form  $2ik_1 + 2qj + c_2$  where  $c_2$  is independent of  $i$  and  $j$ .

CLAIM 3: If  $iL + k_2 \leq j \leq (i+1)L - 1$  and  $k = qL + k_1$  where  $k_1, k_2$  are as above, then

$$p(j+k) - p(j) = -2ik_2 + 2\tilde{q}j - 2\tilde{q}k_2 + L\tilde{q}^2 + A\tilde{q}$$

where  $\tilde{q} = q + 1$ . This is of the form  $-2ik_2 + 2\tilde{q}j + c_3$  where  $c_3$  is independent of  $i$  and  $j$ .

Claims 2 and 3 are proved in the appendix.

We then have

$$\begin{aligned} \gamma_k &= \sum_{i=0}^{M-1} \sum_{j=iL}^{iL+k_2-1} \zeta_{2M}^{p(j+k)-p(j)} + \sum_{i=0}^{M-1} \sum_{j=iL+k_2}^{(i+1)L-1} \zeta_{2M}^{p(j+k)-p(j)} \\ &= \zeta_{2M}^{c_2} \sum_{i=0}^{M-1} \zeta_{2M}^{2ik_1} \sum_{j=iL}^{iL+k_2-1} \zeta_{2M}^{2qj} + \zeta_{2M}^{c_3} \sum_{i=0}^{M-1} \zeta_{2M}^{-2ik_2} \sum_{j=iL+k_2}^{(i+1)L-1} \zeta_{2M}^{2\tilde{q}j} \\ &= \zeta_{2M}^{c_2} \sum_{i=0}^{M-1} \zeta_{2M}^{2ik_1} \sum_{j'=0}^{k_2-1} \zeta_{2M}^{2q(iL+j')} + \zeta_{2M}^{c_3} \sum_{i=0}^{M-1} \zeta_{2M}^{-2ik_2} \sum_{j'=k_2}^{L-1} \zeta_{2M}^{2\tilde{q}(iL+j')} \\ &= \zeta_{2M}^{c_2} \sum_{i=0}^{M-1} \zeta_{2M}^{2i(k_1+qL)} \sum_{j'=0}^{k_2-1} \zeta_{2M}^{2qj'} + \zeta_{2M}^{c_3} \sum_{i=0}^{M-1} \zeta_{2M}^{2i(\tilde{q}L-k_2)} \sum_{j'=k_2}^{L-1} \zeta_{2M}^{2\tilde{q}j'} \\ &= \zeta_{2M}^{c_2} \cdot \sum_{i=0}^{M-1} \zeta_{2M}^{2ik} \cdot \sum_{j'=0}^{k_2-1} \zeta_{2M}^{2qj'} + \zeta_{2M}^{c_3} \cdot \sum_{i=0}^{M-1} \zeta_{2M}^{2ik} \cdot \sum_{j'=k_2}^{L-1} \zeta_{2M}^{2\tilde{q}j'} \\ &= \zeta_{2M}^{c_2} \cdot \sum_{i=0}^{M-1} \zeta_M^{ik} \cdot \sum_{j'=0}^{k_2-1} \zeta_M^{qj'} + \zeta_{2M}^{c_3} \cdot \sum_{i=0}^{M-1} \zeta_M^{ik} \cdot \sum_{j'=k_2}^{L-1} \zeta_M^{\tilde{q}j'} \\ &= \zeta_{2M}^{c_2} \cdot 0 \cdot \sum_{j'=0}^{k_2-1} \zeta_M^{qj'} + \zeta_{2M}^{c_3} \cdot 0 \cdot \sum_{j'=k_2}^{L-1} \zeta_M^{\tilde{q}j'} = 0 \end{aligned}$$

where we have used Lemma 3.1. (The hypotheses of Proposition 4.2 say that  $k$  is not a multiple of  $L$  and hence not a multiple of  $M$ .) We also have, by similar manipulations,

$$\begin{aligned}
\alpha_k &= \sum_{i=0}^r \sum_{j=iL}^{iL+k_2-1} \zeta_{2M}^{p(j+k)-p(j)} + \sum_{i=0}^{r-1} \sum_{j=iL+k_2}^{(i+1)L-1} \zeta_{2M}^{p(j+k)-p(j)} \\
&= \dots \\
&= \zeta_{2M}^{c_2} \cdot \sum_{i=0}^r \zeta_M^{ik} \cdot \sum_{j'=0}^{k_2-1} \zeta_M^{qj'} + \zeta_{2M}^{c_3} \cdot \sum_{i=0}^{r-1} \zeta_M^{ik} \cdot \sum_{j'=k_2}^{L-1} \zeta_M^{\tilde{q}j'}
\end{aligned}$$

which implies

$$|\alpha_k| = \left| \sum_{i=0}^r \zeta_M^{ik} \right| \left| \sum_{j'=0}^{k_2-1} \zeta_M^{qj'} \right| + \left| \sum_{i=0}^{r-1} \zeta_M^{ik} \right| \left| \sum_{j'=k_2}^{L-1} \zeta_M^{\tilde{q}j'} \right|. \quad (1)$$

Now suppose we are in the special case  $L = M$ . Note that  $0 \leq q \leq M-1$ . If  $q = 0$ , then  $k < L$ , so  $|\alpha_k| < k < L = M$ . If  $q = M-1$ , then  $r = 0$ , so  $N - k < L$ , so  $|\alpha_k| < N - k < L = M$ . So assume  $1 \leq q \leq M-2$ , implying  $2 \leq \tilde{q} \leq M-1$ . Then neither  $q$  nor  $\tilde{q}$  is a multiple of  $M$ . Lemma 3.1 then gives us

$$\begin{aligned}
\sum_{j'=0}^{L-1} \zeta_M^{qj'} &= \sum_{j'=0}^{M-1} \zeta_M^{qj'} = 0, \\
\sum_{j'=0}^{L-1} \zeta_M^{\tilde{q}j'} &= \sum_{j'=0}^{M-1} \zeta_M^{\tilde{q}j'} = 0,
\end{aligned}$$

which then implies

$$\begin{aligned}
\left| \sum_{j'=0}^{k_2-1} \zeta_M^{qj'} \right| &= \left| \sum_{j'=k_2}^{L-1} \zeta_M^{qj'} \right| \leq \min\{k_1, k_2\}, \\
\left| \sum_{j'=0}^{k_2-1} \zeta_M^{\tilde{q}j'} \right| &= \left| \sum_{j'=k_2}^{L-1} \zeta_M^{\tilde{q}j'} \right| \leq \min\{k_1, k_2\}.
\end{aligned}$$

Next, observe that we have  $\delta(k, M) = \delta(k, L) = \min\{k_1, k_2\}$ . If we let  $k' = \min\{k_1, k_2\}$ , then Corollaries 3.2 and 3.3 give us

$$\left| \sum_{i=0}^r \zeta_M^{ik} \right| \leq \left| \csc \frac{\pi k}{M} \right| \leq \frac{M}{2k'},$$

$$\left| \sum_{i=0}^{r-1} \zeta_M^{ik} \right| \leq \left| \csc \frac{\pi k}{M} \right| \leq \frac{M}{2k'},$$

Then inequality (1) implies

$$|\alpha_k| \leq \frac{M}{2k'} \cdot k' + \frac{M}{2k'} \cdot k' = M,$$

which completes the proof of Proposition 4.2.

In the case  $L \neq M$ , it is less clear how to bound  $\left| \sum \zeta_M^{qj'} \right|$  and  $\left| \sum \zeta_M^{\tilde{q}j'} \right|$ . We can bound them by  $L$ , but that does not make it obvious whether  $|\alpha_k|$  can be bounded by a multiple of  $\sqrt{N}$ . A more careful analysis may be needed.

In summary, Propositions 4.1 and 4.2 together imply that every LM sequence satisfies  $\gamma_k = 0$  for all  $k \neq 0$ , i.e. every LM sequence is a perfect sequence. In the special case  $L = 1$  (which includes the Chu sequences),  $k$  is always a multiple of  $L$ , so Proposition 4.1 always applies, and the LM sequence has PSL at most  $\sqrt{N/2}$ . In the special case  $L = M$  (which includes the Frank sequences), the LM sequence has PSL at most  $\sqrt{N}$ .

## 5 Appendix

As before,  $L$  and  $M$  are positive integers satisfying  $L|M$ , and  $A \equiv LM \pmod{2}$ . For all nonnegative integers  $j$ , we define

$$s_j = \left\lfloor \frac{j}{L} \right\rfloor,$$

$$t_j = j - L \left\lfloor \frac{j}{L} \right\rfloor,$$

$$p(j) = 2s_j t_j + L s_j^2 + A s_j.$$

Proof of Claim 1. If  $iL \leq j \leq (i+1)L - 1$  and  $k = qL$ , then

$$(i+q)L \leq j+k \leq (i+q+1)L - 1,$$

so we have

$$\begin{aligned} s_j &= \left\lfloor \frac{j}{L} \right\rfloor = i, \\ s_{j+k} &= \left\lfloor \frac{j+k}{L} \right\rfloor = i+q, \\ t_j &= j - Li, \\ t_{j+k} &= (j+k) - L(i+q) = j - Li = t_j, \\ s_{j+k} - s_j &= q, \\ s_{j+k}^2 - s_j^2 &= (i+q)^2 - i^2 = 2iq + q^2, \\ s_{j+k}t_{j+k} - s_jt_j &= (s_{j+k} - s_j)t_j = q(j - Li). \end{aligned}$$

So then

$$\begin{aligned} p(j+k) - p(j) &= 2(s_{j+k}t_{j+k} - s_jt_j) + L(s_{j+k}^2 - s_j^2) + A(s_{j+k} - s_j) \\ &= 2q(j - Li) + L(2iq + q^2) + Aq \\ &= 2qj + Lq^2 + Aq. \end{aligned}$$

Proof of Claim 2. If  $iL \leq j \leq iL + k_2 - 1$  and  $k = qL + k_1$ , and  $k_1, k_2$  are positive integers satisfying  $k_1 + k_2 = L$ , then

$$(i+q)L + k_1 \leq j+k \leq (i+q+1)L - 1,$$

so we have

$$\begin{aligned} s_j &= \left\lfloor \frac{j}{L} \right\rfloor = i, \\ s_{j+k} &= \left\lfloor \frac{j+k}{L} \right\rfloor = i+q, \\ t_j &= j - Li, \\ t_{j+k} &= (j+k) - L(i+q) = j - Li + k_1, \\ s_{j+k} - s_j &= q, \\ s_{j+k}^2 - s_j^2 &= (i+q)^2 - i^2 = 2iq + q^2, \\ s_{j+k}t_{j+k} - s_jt_j &= (i+q)(j - Li + k_1) - i(j - Li) \\ &= ik_1 + qj - qLi + qk_1. \end{aligned}$$

So then

$$\begin{aligned}
p(j+k) - p(j) &= 2(s_{j+k}t_{j+k} - s_jt_j) + L(s_{j+k}^2 - s_j^2) + A(s_{j+k} - s_j) \\
&= 2(ik_1 + qj - qLi + qk_1) + L(2iq + q^2) + Aq \\
&= 2ik_1 + 2qj + 2qk_1 + Lq^2 + Aq.
\end{aligned}$$

Proof of Claim 3. If  $iL + k_2 \leq j \leq (i+1)L - 1$  and  $k = qL + k_1$ , and  $k_1, k_2$  are positive integers satisfying  $k_1 + k_2 = L$ , then

$$(i+q+1)L \leq j+k \leq (i+q+1)L + k_1 - 1.$$

Let  $\tilde{q} = q + 1$ . Then we have

$$\begin{aligned}
s_j &= \left\lfloor \frac{j}{L} \right\rfloor = i, \\
s_{j+k} &= \left\lfloor \frac{j+k}{L} \right\rfloor = i + \tilde{q}, \\
t_j &= j - Li, \\
t_{j+k} &= (j+k) - L(i+q+1) = j - Li - k_2, \\
s_{j+k} - s_j &= \tilde{q}, \\
s_{j+k}^2 - s_j^2 &= (i + \tilde{q})^2 - i^2 = 2i\tilde{q} + \tilde{q}^2, \\
s_{j+k}t_{j+k} - s_jt_j &= (i + \tilde{q})(j - Li - k_2) - i(j - Li) \\
&= -ik_2 + \tilde{q}j - \tilde{q}Li - \tilde{q}k_2.
\end{aligned}$$

So then

$$\begin{aligned}
p(j+k) - p(j) &= 2(s_{j+k}t_{j+k} - s_jt_j) + L(s_{j+k}^2 - s_j^2) + A(s_{j+k} - s_j) \\
&= 2(-ik_2 + \tilde{q}j - \tilde{q}Li - \tilde{q}k_2) + L(2i\tilde{q} + \tilde{q}^2) + A\tilde{q} \\
&= -2ik_2 + 2\tilde{q}j - 2\tilde{q}k_2 + L\tilde{q}^2 + A\tilde{q}.
\end{aligned}$$

## References

- [1] P. Borwein, *Computational excursions in analysis and number theory*. CMS Books in Mathematics, Springer-Verlag, New York (2002).

- [2] D. Chu, *Polyphase codes with good periodic correlation properties*, IEEE Trans. Inf. Theory **IT-18**, 531–532 (1972).
- [3] P. Fan & M. Darnell, *The synthesis of perfect sequences*. In: Cryptography and coding (Cirencester, 1995), Lecture Notes in Comput. Sci. **1025**, 63–73 (1995).
- [4] R. Frank & S. Zadoff, *Phase shift pulse codes with good periodic correlation properties*, IRE Trans. Inf. Theory **IT-8**, 381–382 (1962).
- [5] I. Mercer, *Merit factor of Chu sequences and best merit factor of polyphase sequences*, IEEE Trans. Inf. Theory **59**, 6083–6086 (2013).
- [6] A. Milewski, *Periodic sequences with optimal properties for channel estimation and fast start-up equalization*, IBM J. Res. Dev. **27**, 426–431 (1983).
- [7] W. Mow, *A unified construction of perfect polyphase sequences*. In: IEEE International Symposium on Information Theory, p. 459. IEEE, Whistler (1995).
- [8] W. Mow & S. Li, *Aperiodic autocorrelation and crosscorrelation of polyphase sequences*, IEEE Trans. Inf. Theory **43**, 1000–1007 (1997).
- [9] C. Nunn & G. Coxson, *Best-known autocorrelation peak sidelobe levels for binary codes of length 71–105*, IEEE Trans. Aerosp. Electron. Syst. **44**, 392–395 (2008).
- [10] K. Schmidt, *On a problem due to Littlewood concerning polynomials with unimodular coefficients*, J. Fourier Anal. Appl. **19**, 457–466 (2013).
- [11] K. Schmidt, *Sequences with small correlation*, Des. Codes Cryptogr. **78**, 237–267 (2016).
- [12] R. Turyn, *The correlation function of a sequence of roots of 1*, IEEE Trans. Inf. Theory **IT-13**, 524–525 (1967).